Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report for 02 June 2004

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Associated Press reports security analysts blame insecure passwords for most unauthorized financial transfers, privacy breaches, and even the hacking of corporate networks, and recommend instead using two−factor authentication. (See item 8)
- CNN reports fire broke out on a monorail train carrying passengers to a Memorial Day festival in Seattle, and fire crews hurriedly rescued passengers from smoky cars about one story above ground. (See item 15)
- The South Florida Sun−Sentinel reports U.S. mail service was discontinued in one area in Coral Springs, FL, while police investigated at least four acid bombs found in or near mailboxes. (See item 16)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *June 01, The Christian Science Monitor* — **Power grids prepare for summer heat.** After last summer's blackout that left 50 million customers without electricity, utility companies are increasing efforts reduce the risks of another one as the heat starts to build. Companies are increasing training, spending more money on computer software, adding alarms to unmanned substations, and even hiring helicopters to look for weak spots in their high−tension lines. "We cannot guarantee you will have power, but an outage like last year is highly unlikely," says Bill

Brier of the Edison Electric Institute, an industry trade group. However, **utility executives think it's possible some people may experience a short−term blackout since the utilities will operate more conservatively. If there is even a hint of a local problem that may spread, operators may black out a neighborhood, town, or city to prevent the problem from cascading into something more serious.** In May, the North American Electric Reliability Council (NERC), an industry self−regulatory organization, said it expected the nation to get through the summer without a problem. However, it also warned that extremely hot weather and unanticipated equipment problems might cause some glitches. With the better economy, it is anticipating demand will be 2.5 percent higher than last summer.
Source: http://www.csmonitor.com/2004/0601/p02s01−usgn.html

2. *May 31, New York Times* — **New York utilities recall '03 blackout with fingers crossed.** As the New York region looks toward summer and the first anniversary of the biggest blackout in North American history, two things stand out: there is enough electricity to survive the heat, but the lights may go out anyway. "Unfortunately, until a lot more questions get answered involving what left this region vulnerable, we really can't say that we are fully protected," said Michael C. Calimano, vice president for operations of the New York Independent System Operator, which manages the state's power grid. **More than nine months after the blackout, many industry experts say those same risks remain because the nation as a whole has not significantly improved the interaction of regional power grids. "Positive steps have definitely been taken," said Hoff Stauffer, a senior consultant with Cambridge Energy Research Associates, "but the simple reality is that if a cascade like last summer's blackout starts, it's extremely difficult to stop."** While New York City has sufficient supply in the short term, shortages are on the horizon. Despite the 3,000 megawatts that have been brought online in the last several years, demand in the city is expected to exceed supply by 2009.
Source: http://www.nytimes.com/2004/05/31/nyregion/31power.html?ex=1086667200&en=70275cf45b20757b&ei=5062

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *June 01, Boston Globe* — **Concerns rise over chemicals as targets.** Homeland Security watchdogs call them “prepositioned weapons of mass destruction” for terrorists: huge tanks of concentrated deadly gases that the chemical industry stores near densely populated areas and that railroads bring through cities en route to somewhere else. **The United States harbors more than 100 chemical facilities where an accident would put more than a million people at risk, according to documents filed with the Environmental Protection Agency.** One is in Boston: A chemical distributor acknowledged in its filing that in a worst−case scenario if a tank holding 180,000 pounds of vinyl acetate −− a highly flammable liquid −− ruptured, it would send a 4.9−mile−long toxic cloud through the city. **The presence of these highly toxic chemicals in the midst of cities may be the most vulnerable point in the nation's defenses. But proposals to reduce that risk by requiring the use of alternative chemicals or rerouting hazardous tankers around a city have faltered.** Fear of such an attack on a chemical facility prompted bipartisan momentum in Congress after the September 11, 2001, attacks for requiring the chemical industry to switch to less dangerous processes where

possible. Nevertheless, nearly three years later, the laws regulating chemical plants remain the same as before September 11.
Source: http://www.boston.com/news/nation/washington/articles/2004/06/01/concerns_rise_over_chemicals_as_targets/

4. *June 01, PR Newswire* — **BNSF recognized for promoting chemical transportation emergency preparedness efforts. The Burlington Northern and Santa Fe Railway Company (BNSF) on Tuesday, June 1, announced that it has received the 2003 National Achievement Award from TRANSCAER®.** TRANSCAER®, which stands for Transportation, Community Awareness and Emergency Response, is a nationwide community outreach program designed to promote chemical transportation emergency preparedness and awareness in communities. TRANSCAER® fosters partnerships among chemical producers, distributors, carriers, first responders and government agencies. **Working in conjunction with federal agencies, such as the Environmental Protection Agency, BNSF provided railroad emergency response and hazardous materials awareness training to more than 4,600 emergency responders in more than 20 states.** "BNSF is committed to ensuring the emergency responders in the communities we serve have top−notch training and updated skills to assist in public safety efforts," said Denis Smith, BNSF vice president, Industrial Products Marketing. A subsidiary of Burlington Northern Santa Fe Corporation, BNSF operates one of the largest railroad networks in North America, with about 32,500 route miles covering 28 states and two Canadian provinces.
Source: http://biz.yahoo.com/prnews/040601/datu032_1.html

[Return to top]

Defense Industrial Base Sector

5. *June 01, Aerospace Daily & Defense Report* — **European defense industry in trouble, RAND says.** The European defense industry is in trouble and won't be much of a player in the global defense market, according to a recent report from the RAND Corp. "The European defense industry is hobbled by accessible home markets that are mostly stagnant, with no harmonized procurement, making it a painfully slow and risky process to launch large new projects," says the report. "Access to the world's largest market, the United States, is restricted for most players, while lingering national preference and governmental policy interventions limit the scope of further consolidation within Europe." **European governments aren't likely to procure in joint fashion quickly enough to provide a stable, united European home market for the largest defense industry companies, according to RAND. If things continue, European companies likely will fall behind technologically and U.S. companies increasingly will dominate the industry,** the report says. Report: http://www.rand.org/publications/MG/MG144/MG144.pdf
Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/eur06014.xml

6. *May 30, Honolulu Star−Bulletin* — **The Navy's newest minisub is operational after nearly three years of testing.** During its nearly three years of testing, the Navy's newest special−operations minisub would slip into Pearl Harbor waters at night to clandestinely survey the Pacific Fleet at anchor. "We did it at least three times during the testing period, and they

never detected us ... and I know they were looking for us," said Lt. Cmdr. Jeff Eggers, operations officer for SEAL Delivery Vehicle Team 1. There is only one battery−powered, 65−foot black minisub, called the Advanced SEAL Delivery System (ASDS). The cigar−shaped minisub, which weighs 60 tons, is big enough to accommodate up to 16 SEALs, including two operators who don't have to slip into scuba gear until they are ready to start their mission. Like a submarine, the ASDS vehicle has its own life−support and propulsion systems. "However, unlike a submarine, it is not intended for long−range oceans transits," Eggers said. **The minisub's goal is to deliver a team of Navy special−operations SEALs and their equipment any place in the world, keeping them in a warm and dry environment as long as possible. After nearly three years of deep−water testing in Hawaii, it became operational in September.**
Source: http://starbulletin.com/2004/05/30/news/story9.html

[Return to top]

Banking and Finance Sector

7. *June 01, Today (Philippines)* — **Philippines to stay on money−laundering blacklist this year.** The Philippine government's wish to have the country removed this year from the international blacklist of money laundering−friendly countries will not be granted by the influential Financial Action Task Force (FATF) due to delays in complying with the group's requirements. Bangko Sentral ng Pilipinas (BSP) Governor Rafael Buenaventura, who also chairs the Anti−Money Laundering Council, said the FATF executive committee is still reviewing the law's implementing rules and regulations which the government submitted earlier this year. The central bank chief said the delisting will likely happen next year instead of this year as earlier hoped. **FATF considers the Philippines to be part of a group of noncooperative countries and territories where money laundering may either be rampant or relatively easy to perpetrate. Before a law was passed in 2001, money laundering was not considered a crime in the Philippines.** The Philippine government's failure to have the country removed from the notorious blacklist means more advanced economies like the United States and United Kingdom will have to continue scrutinizing international financial transactions going to and coming from the Philippines.
Source: http://www.abs−cbnnews.com/NewsStory.aspx?section=BUSINESS&o id=52174

8. *June 01, Associated Press* — **Hacking sparks need for complex passwords.** As more Websites demand passwords, scammers are getting cleverer about stealing them. The tools of password harvesting are many, including keystroke recorders secretly installed at public Internet terminals that can capture passwords, and "phishing" e−mails designed to trick users into submitting sensitive data to fraudulent sites that look authentic. There are computer viruses programmed to harvest passwords as well as software that guesses passwords by running through words in dictionaries. **Though analysts have no hard figures on password−specific fraud, they blame insecure passwords for unauthorized financial transfers, privacy breaches and even the hacking of corporate networks. However, with two−factor authentication, having a password alone is useless, but in the U.S., use of two−factor authentication remains limited.** "There's a delicate balance between maintaining security but also providing customers with ease of use," said Doug Johnson, senior policy analyst at the American Bankers Association. Gartner analyst Avivah Litan said banks are "all afraid of

making the first step. They don't want consumers going to other banks because it's too hard." U.S. banks and e−commerce companies have focused, for now, on making sure passwords are strong.
Source: http://www.nytimes.com/aponline/technology/AP−Beyond−Passwor ds.html

9. *May 31, MosNews (Russia)* — **Another Russian bank loses license over money laundering.** The Central Bank of Russia announced its decision to recall the general banking license from the commercial, privately−owned Novocherkassk City Bank. The license was recalled on Saturday, May 29. **The Central Bank (CB) accused Novocherkassk City Bank of numerous violations of the "law on Counteraction of Money Laundering and Sponsorship of Terrorism."** The CB also blames the bank for failing to satisfy cash claims from the creditors and to carry out obligatory payments. Additionally, the bank's management is accused of falsifying returns' data and of failing to comply with a number of laws which regulate banking activities.
Source: http://www.mosnews.com/money/2004/05/31/cblicenserecall.shtm l

[Return to top]

Transportation Sector

10. *June 01, Los Angeles Times* — **Air marshals stick out like sore thumb.** The element of surprise may be crucial to their mission, but it turns out they're "as easy to identify as a uniformed police officer," the Federal Law Enforcement Officers Association said in a complaint to Congress. The problem is not security leaks. It's the clothes. In an era when "dressing down" is the traveler's creed, air marshals must show up in jackets and ties, hair cut short, bodies buffed, shoes shined. **And the tipoff provided by their appearance is magnified by a set of boarding procedures that make them conspicuous. Since they're armed, the marshals can't go through the initial security screening with the rest of the passengers. Instead using the entry points set aside for airport employees, however, the marshals often must go through the "exit" lanes −− marching against the flow of arriving passengers, at times in full view of travelers.** "They lose the advantage" of being undercover, said John Amat, a spokesman for the marshals within the federal law officers group. The air marshal service has grown from about 30 officers at the time of the September 11 terrorist attacks to several thousand today, operating under a $600 million annual budget.
Source: http://www.trivalleyherald.com/Stories/0,1413,86~10669~21847 39,00.html

11. *June 01, News.scotsman.com* — **BA continues flights to terror−hit country. British Airways (BA) flights to terrorist−hit Saudi Arabia are to carry on for the time being, the airline said Tuesday, June 1. BA suspended flights to the Middle Eastern kingdom last year but is continuing with four flights a week to both Riyadh and Jeddah.** “It’s business as usual, but we are keeping a close watch on the official Foreign Office travel advice,” a BA spokesman said. He added that there was, as yet, no indication that London−bound flights from Saudi Arabia were any busier than normal with British nationals wishing to return home. The Foreign Office is currently advising Britons against “all but essential travel to Saudi Arabia." There are several thousand Britons in Saudi Arabia −− most of them residents who are working there.
Source: http://news.scotsman.com/latest.cfm?id=3004551

12. *June 01, Associated Press* — **Truckers helping prevent terrorism on highways. Highway Watch is a federally−funded Department of Homeland Security program that recruits those most familiar with highways and byways to look for the out−of−place or unusual.** The American Trucking Association (ATA) is leading the effort under a two−month−old agreement with the Transportation Security Administration (TSA). The government is providing $19.3 million for the program this year and $22 million in 2005, money meant to offset the expense of training by law enforcement officials. **Arkansas was the first state to incorporate the anti−terror training, through the Arkansas Trucking Association.** Group spokesperson Lane Kidd said Highway Watch was initially conceived by the federal Motor Carrier Safety Administration as a safety network, with truckers reporting accidents to help lower response times and report drunk drivers and stranded motorists. **Kidd, who is a Highway Watch member, said the four−hour training course includes lectures and video and focuses on spotting things that are out−of−place and possibly indicative of terrorist activity.** TSA spokesperson Andrea Fuentes said the program is being expanded to include a host of others who work with transportation infrastructure: mass transit workers, bridge and maintenance workers, toll booth attendants and others.
Source: http://www.baxterbulletin.com/news/stories/20040601/localnew s/547935.html

13. *June 01, The Muskegan Chronicle (MI)* — **Much−anticipated ferry arrival re−links port cities.** The electronic tone of the Lake Express ship's horn sounded the beginning of a new era for cross−lake ferry service between Muskegon and Milwaukee, WI, Tuesday morning, June 1. For the first time since 1970, passengers and vehicles are being carried between the two historically linked port cities. The Lake Express is a new high−speed catamaran that can cross the lake in two and one−half carrying 250 passengers and 46 vehicles. It has high−tech features aimed at eliminating seasickness, and offers cell phone and Internet service to passengers. **The Coast Guard plans to have officers aboard both the Lake Express ferry and the SS Badger out of Ludington throughout the summer because of heightened federal security provisions,** Lt. Jamie Rickerson said. The Guard also does other waterway patrols and onshore safety patrols.
Source: http://www.mlive.com/news/muchronicle/index.ssf?/base/news−4 /1086104701156940.xml

14. *June 01, Associated Press* — **Travelers face long lines at Georgia airport. Thousands of frustrated travelers snaked through an overwhelmed Hartsfield−Jackson Atlanta International Airport on Tuesday, June 1, waiting in two−hour−long lines to pass through security checkpoints.** Lines at one of the country's busiest airports nearly spilled onto the sidewalks outside. Fliers stood in a labyrinthine line that wound through ticketing, baggage claim and a food court before even nearing the security gate. The delay was caused by a rush of business and holiday travelers. Hartsfield−Jackson officials have warned for many months they could not handle the summer travel crush without extra help from the federal Transportation Security Administration. The airport asked for more security lanes, but the additions haven't been completed. All of the airport's 18 security checkpoints were in use Tuesday. Hartsfield−Jackson's passenger count this year is expected to top 81 million people, exceeding its record year in 2000.
Source: http://www.newsday.com/news/nationworld/nation/wire/sns−ap−a irport−lines,0,7140531.story?coll=sns−ap−nation−headlines

15. *June 01, CNN* — **Monorail train catches fire in Seattle. A monorail train carrying passengers to a Memorial Day festival caught fire Monday afternoon, May 31, in Seattle, WA, and fire crews hurriedly rescued passengers from smoky cars about one story above ground.** At least five people were taken to Harborview Medical Center where they were being evaluated, a nursing supervisor said. "There was a pop and then we started seeing smoke," a shaken female passenger holding a child told KIRO−TV, a CNN affiliate. Asked if she felt in danger before rescuers arrived, the woman said, "We all did." Dozens of emergency crews were on the scene. Firefighters used ladders, including one ladder truck, to reach the smoking train. Dozens of passengers crowded the open doors of the monorail awaiting rescue. **It was not immediately clear what caused the fire and an investigation has been launched.** Glenn Barney, general manager of the Seattle Center Monorail, said he did not know what caused the fire. **He said each monorail train can hold as many as 450 passengers.** The monorail travels a mile between downtown Seattle and the Seattle Center Fairgrounds where the annual Memorial Day Folklife Festival was taking place.
Source: http://www.cnn.com/2004/US/West/05/31/monorail.fire/index.ht ml

[Return to top]

Postal and Shipping Sector

16. *June 01, South Florida Sun−Sentinel* — **Mail service cut off after bombs found. Mail service was discontinued in one area on Tuesday, June 1, while police investigated at least four acid bombs found in or near mailboxes in Coral Springs, FL.** Sgt. Nick Nicorvo, police spokesman, said Tuesday's, June 1, four cases join four other acid bomb reports that have occurred in the past week. A postal inspector said no mail would be delivered on North Springs Way until Wednesday, June 2. No injuries have been reported from any of the eight incidents. The Broward County, FL, Sheriff's Office Bomb Squad was called in to help police. Mailboxes were being searched individually in the affected areas. All incidents have occurred within a half−mile to three−quarters of a mile of each other.
Source: http://www.sun−sentinel.com/news/local/broward/sfl−61acidbom bs,0,2599920.story?coll=sfla−news−broward

17. *May 31, ComputerWorld* — **Postal Service single sign−on technology. The U.S. Postal Service (USPS) this summer plans to complete the installation of a single sign−on system that will support about 155,000 end users and more than 7,000 applications and Websites.** The new system has already been rolled out to 147,000 users, and Bob Otto, chief technology officer at the USPS, said last week that the 11−month rollout is due to be finished in August. The new system lets USPS workers log onto 1,000 internal applications and 6,000 external ones using only their Windows passwords, Otto said. "An average end user had five to 10 different log−on IDs and passwords, and they wrote them," Otto said. "That was a big security issue." In addition, calls to the help desk by end users who had forgotten their passwords were costing the USPS millions of dollars per year in operating costs, according to Otto.
Source: http://www.computerworld.com/softwaretopics/software/apps/st ory/0,10801,93515,00.html

[Return to top]

Agriculture Sector

18. *June 01, Xinhuanet* — **Immunity to mad cow disease. A Japanese beer maker has succeeded in producing a cow that is immune to mad cow disease, but experts said it was too early for livestock producers to celebrate.** The company said it has produced, jointly with a U.S. company, a cow that carried none of the prion proteins that cause the brain−wasting disease, also known as bovine spongiform encephalopathy or BSE. BSE is passed on by an infectious protein particle called a prion, a misshapen protein that can convert other proteins to the deadly form by touching them. The two firms plan to use the cow to develop medicines for diseases such as hepatitis C, pneumonia, and rheumatism. The animal, produced through genetic engineering, is still in its mother's womb and is expected to be born early next year.
Source: http://news.xinhuanet.com/english/2004−06/01/content_1501436 .htm

19. *June 01, Herald (United Kingdom)* — **Infection ravages fish farms. An infectious wasting disease is sweeping through Scottish salmon farms, affecting seven out of 10 marine sites, according to the latest official figures.** Infectious pancreatic necrosis (IPN) can kill up to a third of young fish, posing a huge economic threat to the Scottish industry. A working group set up by the Scottish Executive, whose conclusions have been circulated throughout the industry recently, has reported clear evidence that IPN is increasing in seawater sites in most regions. **The report concludes that little can be done until a vaccine is available and that current movement restrictions on infected fish farms are inadequate to control the disease.** The working group reported that prevalence rates −– the proportion of tests giving a positive result for the virus −– had increased from less than 50 percent in 2000 to 82 percent in 2002, the most recent figure.
Source: http://www.theherald.co.uk/news/17185.html

20. *June 01, USAgNet* — **Program set to track livestock. Northwest beef industry leaders plan to implement a pilot animal identification system in six Western states, aimed at ensuring that a diseased animal or tainted meat can be traced within 48 hours.** Cattlemen, feedlot owners, and meat packers hope the system will serve as a model for a national identification system. Industry groups in Washington, Oregon, Idaho, Utah, Nevada, and California have signed on to the pilot program. The project will enroll about 12,000 cattle in the next two to three years, slowly adding bison and sheep to the system, chairman of the program, Rick Stott, said Friday, May 28. "The primary objective of the project itself is to find a workable, manageable and the least expensive way for producers to implement the animal ID system that's being proposed" by the U.S. Department of Agriculture, said Stott.
Source: http://www.usagnet.com/story−national.cfm?Id=578&yr=2004

21. *June 01, Kentucky Ag Connection* — **Wheat disease in Kentucky.** A disease that can cause serious damage to winter wheat has been reported in several areas of Kentucky. **Fusarium head blight, also known as head scab, has been seen in some fields in southern and western Kentucky. It is common to see 30 to 50 percent incidences in some fields in Christian, Todd and Logan counties,** said Don Hershman, a plant pathologist with the University of Kentucky College of Agriculture. In McLean County, several fields were reported to be approaching 80 percent. "At this time I really do not know the full extent of Fusarium head blight statewide," Hershman said. Fusarium head blight appeared in many wheat fields across the commonwealth in 2003 in the highest levels since 1991 and much of Kentucky 's

wheat crop had high levels of DON, or vomitoxin. DON is a toxin produced by the fungus as it is infecting and developing in the wheat heads. Excess DON can seriously impact a farmer's ability to sell his crop in some markets.
Source: http://www.kentuckyagconnection.com/story−state.cfm?Id=261&y r=2004

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

22. *June 01, Beacon Journal (OH)* — **Researchers working to guard water supply.** Detecting a bioterrorist attack on the nation's water supply could take several hours, if not days, and require highly trained technicians and equipment costing hundreds of thousands of dollars. Researchers, however, are pretty sure they can whittle that wait down to minutes, with easy−to−use, hand−held devices costing a few thousand dollars. **With a $796,520 grant from the U.S. Department of Homeland Security, the researchers at Kent State University and the Northeastern Ohio Universities College of Medicine (NEOUCOM) are using liquid−crystal technology −− best known for putting numbers on digital watches or images on computer screens −− to detect bacteria or viruses.** "What we're really doing now is taking that concept, that idea, and putting the nuts and bolts around it," said Gary Niehaus of NEOUCOM. "Ideally, we're looking at detection within five minutes. That's what our goal is. And we would be happy with 15 minutes, but that's the range we're looking at." **It now takes anywhere from eight to 48 hours to identify the presence of pathogens. Cutting that time would allow people exposed to the pathogens to get the proper treatment sooner.**
Source: http://www.ohio.com/mld/beaconjournal/news/local/8807845.htm ?1c

23. *May 31, South Florida Sun−Sentinel* — **Water managers to test deep−wells for excess rainwater storage.** South Florida can see 50−plus inches a year. The problem at hand: how to capture and hold onto the rainwater excess, runoff carried away by canals to prevent flooding. Federal and state water managers want to tackle that with an innovative idea. **It calls for 333 wells stretching from southwest Palm Beach County to Lake Okeechobee designed to drink down and store a potential 1.6 billion gallons of water pulled from canals and reservoirs in times of plenty.** Before embarking on the plan, they intend to first establish seven test wells at different locations. The intention is to explore "technical uncertainties" in their $1.7 billion proposal to bank all that water 1,000 feet underground, inside a rock sponge called the Floridan Aquifer. If the wells, utilizing a 35−year−old idea but on an unprecedented scale, work as hoped, they could help replenish city drinking−water supplies, irrigate farmland, and nourish natural areas while requiring little land for a voluminous water return, the district and Corps of Engineers say.
Source: http://www.sun−sentinel.com/news/local/southflorida/sfl−pwel ls31may31,0,4322292.story?coll=sfla−home−headlines

[Return to top]

Public Health Sector

24. *June 01, Medical News Today* — **Usefulness of bioterrorism surveillance systems. Although surveillance systems to detect illnesses and syndromes related to bioterrorism have proliferated, researchers found little information about how good they would be at detecting bioterrorism and emerging infections.** Researchers identified 115 systems that collect various surveillance reports. Only three had been evaluated for accuracy. Only two disease surveillance systems and no environmental monitoring system had been evaluated in studies published in peer−reviewed journals. "Given the striking lack of information on the timeliness, sensitivity and specificity, and ability of systems to facilitate decision making, clinicians and public health officials deploying these systems do so with little scientific evidence to guide them," the authors say.
Source: http://www.medicalnewstoday.com/index.php?newsid=8926

25. *June 01, Reuters* — **Ebola vaccine. A Dutch biotechnology firm said on Tuesday, June 1, that a single dose of its Ebola vaccine has successfully protected monkeys from the deadly disease in trial tests.** The company, which used its PER.C6 gene technology to develop the vaccine, said in a statement the monkey experiments were performed over the last six months by the Vaccine Research Center (VRC) of the U.S. National Institute of Allergy and Infectious Diseases (NIAID). PER.C6 gene technology uses human cells as a platform to produce drugs, including vaccines, to battle HIV and cancer.
Source: http://www.forbes.com/infoimaging/newswire/2004/06/01/rtr139 0495.html

26. *June 01, Globe and Mail (Canada)* — **Disaster mass burial may be unnecessary.** The notion that dead bodies that pile up during floods, earthquakes, and other calamities will spawn outbreaks of infectious disease is widely accepted, but it's not true, according to new research. **"There is no evidence that, following a natural disaster, dead bodies pose a risk of epidemics,"** said Oliver Morgan of the London School of Hygiene and Tropical Medicine. In a paper published in the June 2 edition of the Pan American Journal of Public Health, he notes that victims of natural disasters usually die of trauma and are highly unlikely to have serious infectious diseases. The same is true of victims of war. **And even in instances when mass fatalities have resulted from epidemic outbreaks of diseases such as the plague, cholera, or smallpox, the infectious agents do not survive in the body very long after death.**
Source: http://www.theglobeandmail.com/servlet/ArticleNews/TPStory/LAC/20040601/HDISASTERS01/TPHealth/

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

27. *June 01, NBC11.com (CA)* — **CHP to hire new officers. The California Highway Patrol (CHP) will hire at least 270 new officers to help deal with terrorist threats.** CHP Commissioner D.O. "Spike" Helmick said recently **the extra demands of protecting California from terrorism and a far−reaching order to leave vacancies unfilled had strained the patrol's ability to ensure safety on roadways.** "We are doing more work with 90 officers less than prior to September 11, 2001," Helmick told lawmakers. The current budget gives the CHP an authorized force of 6,136 officers, but the agency is operating at about 90 fewer than full strength. Of that force, 5,373 are assigned to road duty.
Source: http://www.nbc11.com/politics/3368585/detail.html

[Return to top]

Information Technology and Telecommunications Sector

28. *June 01, Associated Press* — **Many wireless networks lack security.** With a laptop perched in the passenger seat of his car and a special antenna on the roof, Mike Outmesguine ventured off to check out wireless networks between Los Angeles and San Francisco. **While his 800−mile drive confirmed that the number of wireless networks is growing explosively, he also found that only a third used basic encryption a key security measure. In fact, in nearly 40 percent of the networks not a single change had been made to the gear's wide−open default settings.** Experts say that while Wi−Fi hardware makers have made initial setup easy, the enabling of security is anything but. Meanwhile, average users are no longer tech savvy. The gadgets are mainstream, appearing on the shelves of Wal−Mart and other mass retailers. During his drive, Outmesguine counted 3,600 hot spots, compared with 100 on the same route in 2000. The result? A lot of wide−open networks that offer anyone within range of the Wi−Fi signal free access to a high−speed Internet connection. Any hacking is unlikely to be noticed, while illegal activity would be traceable only to the name on the Internet account.
Source: http://abcnews.go.com/wire/US/ap20040601_368.html

29. *June 01, CNET News.com* — **Study: Dipping costs to fuel corporate VoIP growth.** The number of corporate telephone lines that use voice over Internet Protocol (VoIP) will leap from 4 percent to 44 percent by 2008, fueled by reduced equipment costs, according to a new study. Corporate spending on VoIP also will rise from this year's expected $1 billion to $5.5 billion by 2008, said Teney Takahashi, an analyst at the Radicati Group, which on Tuesday released the study, called "Corporate VoIP Market: 2004−2008." **The main reason for VoIP growth among corporations is the plunging cost of outfitting an office with VoIP**, Takahashi said. Over the next four years, leading vendors will lower their own manufacturing costs as they become more adept at making VoIP equipment. **By 2008, it should cost corporations only about $75 to $600 per line, down dramatically from the current $375 to $1,000 per line**, he said. The biggest winners will continue to be equipment vendors that sell hybrid systems, which combine VoIP with traditional circuit switches. But these companies will see their current share of the market, nearly 92 percent, drop to 70 percent by 2008, as smaller companies upgrade to pure VoIP systems, he said. Additional information about the study is available here: http://www.radicati.com/reports/single.shtml
Source: http://news.com.com/Study%3A+Dipping+costs+to+fuel+corporate+VoIP+growth/2100−7352_3−5223666.html?tag=nefd.top

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

Watch Synopsis: The LSASS exploit code for Windows XP has been perfected for some malicious viruses and worms, as the recent versions of the Korgo IRC Worm prove. The Watch still expects that other exploits for MS04−011 announced vulnerabilities will be perfected and used in the future.

Current Port Attacks

Top 10 Target Ports	21 (ftp), 53 (domain), 57 (priv−term), 25 (smtp), 23 (telnet), 22 (ssh), 20 (ftp−data), 66 (sql*net), 1 (tcpmux), 68 (bootpc) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

General Sector

30. *June 01, Associated Press* — **Fire at Commerce Department. Firefighters were called to the Department of Commerce, in Washington, DC, late Monday, May 31, after a fire erupted in the basement of the building, possibly after an electric transformer exploded.** The fire was quickly extinguished, but smoke filled parts of the building, adjacent to the White House, fire officials said. The building was largely unoccupied and no one was injured. However, department spokesperson Dan Nelson said the building would be closed Tuesday, June 1, and only essential employees were expected to report for work. Fire department spokesman Alan Etter said investigators were looking into whether a faulty transformer was to blame for the fire in the building's basement.
Source: http://www.twincities.com/mld/twincities/news/breaking_news/ 8806823.htm?1c

31. *June 01, CBS News* — **Terror suspect eyed hotels according to Department of Justice.** Jose Padilla, a terrorism suspect, sought to blow up hotels and apartment buildings in the United States in addition to planning an attack with a "dirty bomb" radiological device, according to government documents. The documents were released Tuesday, June 1, by the Department of Justice. **"Padilla and the accomplice were to locate as many as three high−rise apartment buildings which had natural gas supplied to the floors," the government summary of interrogations revealed. "They would rent two apartments in each building, seal all the openings, turn on the gas, and set timers to detonate the buildings simultaneously at a later time," the papers alleged.** The documents said al Qaeda officials were skeptical of Padilla's ability to set off a dirty bomb, but were very interested in the apartment operation.

Padilla was to conduct an Internet search on buildings that had natural gas heating, open a bank account and obtain documents needed to rent an apartment. The plot called for blowing up 20 buildings simultaneously, but Padilla said he could not rent multiple apartments under one identity without drawing attention. The FBI arrested Padilla in May 2002 as he returned from a trip to Pakistan.
Source: http://www.cbsnews.com/stories/2004/06/01/terror/main620582. shtml

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer